

Claims

What is claimed as being new and desired to be protected by Letters Patent of the United States as follows:

1. A method and system for preventing unauthorized use of a software product on a host computer system or any other process based hardware in association with a licensing system comprising the steps of:

at the beginning of installation or execution of a software product at a host computer system;

dynamically encrypting a portion of the unique serial number assigned to the software product and transmitting it along with a proper action request to the licensing system;

at the licensing system:

dynamically decrypting the received portion of the serial number and identifying the action requested;

comparing the dynamically decrypted portion of the received serial number with the stored serial number;

if the received portion matches with the stored portion, dynamically encrypting the same or another portion of the stored serial number of the software product along with an action response and transmitting it back to the host computer system;

if the received portion does not match with the stored portion, transmitting an error status message or code back to the host computer system;

at the host computer system:

dynamically decrypting the received portion of the serial number;

comparing the received portion with the stored portion of the serial number;

if the received portion matches with the stored portion, enable execution or proceed with the installation of the software product;

if the received portion does not match with the stored portion, disable the execution or installation of the software product; and

if an error status message or code received, inform the user by displaying the error message.

2. The method and system according to claim 1 wherein the transmitting portion of the software product serial number is randomly selected.

3. The method and system according to claim 1 wherein the method for dynamic encryption/decryption of digital information comprising the steps of:

at the host computer system and the licensing system before the start of encryption/decryption procedure:

means for assigning and mutually agreeing upon a pre-determined number of bits that are located at pre-determined and specific positions, called Function Bits, within a random number consisting of an arbitrary length;

means for defining a function pool containing any type of mathematical or logical functions of any complexity such that there exists a unique inverse mathematical or logical function for each of the functions defined in the said pool;

means for defining a number 'M' which indicates the total number of encryption/decryption rounds.

at the host computer system:

- (a) means for generating a random number R1 of an arbitrary length
- (b) means for identifying and sequentially arranging the pre-determined number of Function Bits located at the pre-determined and specific positions within the random number R1,
- (c) means for sequentially arranging an array of Function Bits;
- (d) means for selecting a set of Function Bits consisting of certain numbers in a pre-determined order;
- (e) means for producing a numeric number value based on the selected Function Bits,
- (f) means of selecting a mathematical or logical function from the function pool based on the numeric number value,
- (g) means for encrypting a digital information segment through operating a mathematical or logical function selected from the function pool as described in step (f); and
- (h) means for repeating step (d) through step (g) for 'M' number of times.

4. The method and system according to claim 3 wherein the Function Bits located within a random number of any length can be uniquely assigned and mutually recognized by the host computer system and the licensing system through the use of any mathematical or logical functions of any complexity.

5. The method and system according to claim 3 wherein the host computer system or the licensing system builds a decryption table, comprising the steps of:

- (a) means for sequentially arranging an array of Function Bits contained in the received random number;
- (b) means for selecting the Function Bits in a pre-determined order;
- (c) means for selecting a mathematical or logical function from the function pool based upon the numeric number value of step (b);
- (d) means for identifying the corresponding inverse function for the mathematical or logical functions as recognized in step (c);
- (e) means for tabulating the identified inverse mathematical or logical function entries;
- (f) means for repeating steps (b) through (e) for 'M' number of times and appending the inverse function entries resulting from each round into a tabular form of a decryption table.

6. The method and system according to claim 1 wherein the said method for dynamic decrypting of digital information between the host computer system and the licensing system or vice versa, the method comprising the steps of:

- (a) means for receiving the encrypted digital information segment;
- (b) means for decrypting the digital information segment with the last inverse mathematical function entry as found in the decryption table built in step (f) of claim 5;
- (c) means for repeating the above step (b) until all the inverse mathematical or logical functions are exhausted as found in the said decryption table;

7. The method and system according to claim 1 wherein the host computer system and the licensing system initializes a dynamic encryption session comprising the steps of:

at the host computer system:

means for generating two random numbers R1 and R2;

means for treating R2 as a data segment and dynamically encrypting R2 through using R1;

means for transmitting R2_(Enc.) and R1 to the licensing system;

at the licensing system:

means for generating two random numbers R3 and R4;

means for treating R4 as a data segment and dynamically encrypting R4 through using R3;

means for transmitting R4_(Enc.) and R3 to the licensing system;

8. The method and system according to claim 1 wherein the host computer system and the licensing system encrypts the digital information segments comprising the steps of:

at the host computer system:

means for encrypting any subsequent digital information segments directed to the licensing system by using R4;

at the licensing system:

means for encrypting any subsequent digital information segments directed to the licensing system by using R2;

9. The method and system according to claim 1 wherein the host computer system and the licensing system establishes decryption session comprising the steps of:

at the host computer system:

means for decrypting the received random number R4 through the use of R3;

means for using the random number R2 to decrypt any digital information segments received from the licensing system;

at the licensing system:

means for decrypting the received random number R2 through the use of R1; and

means for using the random number R4 to decrypt any digital information segments received from the host computer system;

10. The method and system according to claim 3 wherein the method of selecting Function Bits is comprising the steps of:

(a) means for establishing a sliding window selector over an array of Function Bits;

(b) means for selecting a set of a pre-determined number of Function Bits from the said array; and

(c) means for advancing the sliding window selector over the Function Bits array to select another set of Function Bits in a pre-determined order.

11. The method and system according to claim 10 wherein the method of changing the bit values in an array of Function Bits through Insertion Bits, comprising the steps of:

(a) means for defining a pre-determined number and location of Insertion Bits in the shift register containing the array of Function Bits; and

(d) means for changing the bit values of the Insertion Bits.

12. The method and system according to claim 3 wherein the method of selecting the number 'M' which indicates encryption/decryption rounds, comprising the steps of:

(a) means for reading a pre-determined number of bits from an array containing Function Bits and calculating the binary equivalent number; and

(b) means for adding a pre-determined number 'm' into the results of step (a) to determine the number 'M'.

13. The method and system according to claim 1 wherein the licensing system is adapted in a shape of a dongle with the ability to be connected to any port of a host computer system.

14. The method and system according to claim 1 wherein the licensing system is adapted to be installed on a remote computer system in software modules.

15. The method and system according to claim 1 wherein both the host computer system and the licensing system engage in executing fictitious processes, comprising:

at the host computer system:

(a) means for initializing a random number of fictitious processes;

(b) means for transmitting the results to the licensing system;

at the licensing system:

(a) means for establishing filters to block out any fictitious data traffic received from the computer system; and

(b) means for transmitting a string of random numbers to the host computer system.

16. A method and system for distributing credits through a licensing system to a host computer system or any other process based hardware, comprising;

requiring the host computer system to obtain a credit from the licensing system before operating a software product;

requiring the licensing system to decrement the credit availability in any manner after delivering a credit to the host computer system.

17. The method and system according to claim 16 wherein an authorized entity can utilize any method to change the number of available credits in a licensing system.

18. The method and system according to claim 16 wherein a first licensing system adapted in a first form interacts with a second licensing system adapted in a second form, comprising:

(a) means for "downloading " credits required for execution of a software product from the first form of the licensing system to the second form of the licensing system; and

(b) means for "uploading " credits required for execution of a software product from the first form of the licensing system to the second form of the licensing system.

19. The method and system according to claim 16 wherein a licensing system increment credit(s) in its credit pool through uninstalling a software product from a host computer system, comprising the steps of;

at the host computer system:

(a) means for transmitting a credit request to the licensing system during the un-installation process of the software product;

at the licensing system:

(a) means for verifying the un-installation process of the software product to be completed at the host computer system;

(b) if the verification is successful, means for incrementing the credit(s) in the credit pool; and

(c) if the verification fails, means for notifying the user with the proper error message.

20. The method and system according to claim 16 wherein a licensing system can recover credit(s) previously used for an installed software product on a hard drive which has become non-operational, the method comprising the following steps of:

at the host computer system:

(a) means for loading a software program into the computer memory to directly access pre-determined location and number of sectors on the hard drive containing the said software product;

(b) means for establishing a communication session between the said hard drive and the licensing system;

at the licensing system:

(a) means for directly writing a pre-determined set of data information on the said sectors of the hard drive;

(b) means for verifying the written information on the said sectors;

(c) if the verification process is successful, issuing a credit(s) in the credit pool of the licensing system;

(d) if not, generating an error message or code and transmitting it back to the computer system.

21. A method for running a software product on a computer or any other process based hardware, the method comprising the following steps:

transmitting credit request for execution of a software product through using dynamic encryption to a licensing system;

determining if a credit should be released for the execution of the software product by the licensing system;

if yes, releasing the credit through dynamic encryption by the licensing system to the said computer system;

if not, transmitting an error message or code back to the said computer system;

at the host computer system:

executing the software product if a credit is received;

disabling the software product if no credit is received.